IN THE CLAIMS

1. (Canceled)

2. (Previously presented) A method according to claim 45 , wherein the configuration service includes a call center, step (B) involving the user passing said user-related information to the configuration service by communicating with the call center in one of the following ways:
- directly by telephone;
- directly by an electronic messaging system;
- indirectly through a third party who contacts the call center by telephone;
- indirectly through a third party who contacts the call center by an electronic messaging system.

3-9. (Canceled)

10. (Previously presented) A method according to claim 45, wherein the authentication of the connectivity unit to the configuration service involves a cryptographic-based challenge-response interchange conducted between the connectivity unit and configuration service to confirm that the connectivity unit is the possessor of the private key related to the public key passed in the identity-sequence certificate whereby to authenticate the unit as the one bearing the identity sequence included in the certificate.

11. (Previously presented) A method according claim 45, wherein communication between the connectivity unit and configuration service in step (C) is effected across a communications infrastructure that comprises a data network to which the configuration service is connected, and an access network to which the user has a subscriber connection and which provides access to the data network through a data-network access point, the process of establishing a connection

2

between the connectivity unit and the configuration service in step (C) involving the following sub-steps:

(a) - the connectivity unit connects via the user's subscriber connection across the access network to the data-network access point using addressing information for the latter held as part of said configuration communication parameters;

(b) - the data-network access point authorises access by the connectivity unit to the data network on the basis of a username and password which are included in said configuration communications parameters and are passed to the access point by the connectivity unit, the data-network access point effecting this authorisation by using the services of an authorisation server associated with the configuration service ;

(c) - upon access being authorised in step (b), the data-network access point assigns an address for the connectivity unit on the data network and passes this address to the authorisation server which in turn passes it to a configuration manager of the configuration service ; and

(d) - the configuration manager prompted by the step (c) authorisation server contacts the connectivity unit at the assigned address of the latter on the data network in order to download said operational communication parameters to the connectivity unit.

12. (Previously presented) A method according to claim 11, wherein the identity sequence of the connectivity unit is in the user name passed to the authorisation server and is checked by the latter against a database of valid identity sequences, access to the data network only being authorised if the identity sequence included in the user name is a valid one.

13. (Previously presented) A method according to claim 11, wherein the authorisation server is associated with a configuration domain; the username passed by the connectivity unit to the data-network access point being of the form:

3

identity sequence of connectivity unit @ configuration_domain
and the data-network access point recognising the 'configuration_domain' as
indicating the authorisation server to be used and thereupon contacting the latter
over the data network and passing it the identity sequence contained in the
username it received from the connectivity unit.

14-16. (Canceled)

17. (Currently amended) A method according claim ~~14~~5, wherein communication
between the connectivity unit and configuration service in step (C) is effected
across a communications infrastructure that comprises a data network to which
the configuration service is connected, and an access network to which the user
has a subscriber connection and which provides access to the data network
through a data-network access point, the process of establishing a connection
between the connectivity unit and the configuration service in step (C) involving
the following sub-steps:

(a) - the connectivity unit connects via the user's subscriber connection across
    the access network to the data-network access point using addressing
    information for the latter held as part of said configuration communication
    parameters;

(b) - the data-network access point authorises access by the connectivity unit to
    the data network on the basis of a username and password which are
    included in said configuration communications parameters and are passed
    to the access point by the connectivity unit, the data-network access point
    effecting this authorisation by using the services of an authorisation server
    associated with the configuration service;

(c) - upon access being authorised in step (b), the data-network access point
    assigns an address for the connectivity unit on the data network and passes
    this address to the connectivity unit; and

(d) - the connectivity unit contacts the configuration manager over the data
    network at an address held by the connectivity unit as part of said

4

configuration communication parameters, the configuration manager subsequently transmitting said operational communication parameters to the connectivity unit.

18. (Previously presented) A method according to claim 17, wherein the identity sequence of the connectivity unit is included in the user name passed to the authorisation server and is checked by the latter against a database of valid identity sequences, access to the data network only being authorised if the identity sequence included in the user name is a valid one.

19. (Previously presented) A method according to claim 17, wherein the authorisation server is associated with a configuration domain; the username passed by the connectivity unit to the data-network access point being of the form:

identity sequence of connectivity unit @ configuration_domain
and the data-network access point recognising the 'configuration_domain' as indicating the authorisation server to be used and thereupon contacting the latter over the data network and passing it the identity sequence contained in the username it received from the connectivity unit.

20. (Canceled)

21. (Previously presented) A method according to claim 45, wherein at the end of step (C) the configuration service initiates the sending of a wake-up indication to the connectivity unit, the latter responding to receipt of this indication by seeking to connect to the service entity using the said operational communications parameters whereby to check that the connectivity unit has been correctly configured for communication with the service entity.

22. (Canceled)

5

23. (Previously presented) A method according claim 21, wherein communication between the connectivity unit and configuration service in step (D) is effected across a communications infrastructure that comprises a data network to which the configuration service is connected, and an access network to which the user has a subscriber connection and which provides access to the data network through a data-network access point; and wherein an identifier of the subscriber connection on said access network is stored with said user-related information, said wake-up indication taking the form of a call placed to said subscriber connection.

24-30. (Canceled)

31. (Previously presented) A configuration service system for configuring a connectivity unit for communication with a service entity across a communications infrastructure, said connectivity unit having configuration communications parameters pre-installed therein prior to a user taking possession of the unit, a public-key/private-key cryptographic key pair and configuration communication parameters including an identity-sequence certificate linking the public key to an identity sequence of the unit; the configuration service system comprising:

-   a data processing system including a store for holding user-related information;
-   a call center to which user-related information about a new user of a connectivity unit can be passed for entry into the data processing system for storage in said store; the user-related information including the identity sequence of the connectivity unit ; and
-   interface means for interfacing the data processing system with the communications infrastructure whereby to enable communication between the data processing system and the connectivity unit of the new user; access to the data processing system through the interface means requiring knowledge of at least one said configuration communications parameter;

6

the data processing system further including:

- authentication means comprising means for verifying the authenticity of a said identity-sequence certificate passed by a said connectivity unit to the data processing system across the communications infrastructure;

- means for accessing the user-related information held in said store on the basis of a said identity sequence received from a said connectivity unit in a said identity-sequence certificate authenticated by the authentication means, this identity sequence serving to identify the connectivity unit to the data processing system;

- means for deriving for the connectivity unit of said new user, operational communication parameters on the basis of said user-related information, these operational parameters including a user-id certificate associating the public key of the unit with a user identity derived from said user-related information; and

- means for transmitting said operational communications parameters to the connectivity unit operational for use by the latter for communicating with said service entity.

32. (Canceled)

33. (Previously presented) A configuration service system according to claim 31, wherein the authentication means further comprises means for effecting a cryptographic-based challenge-response interchange between the connectivity unit and data processing system whereby to confirm that the connectivity unit is the possessor of the private key related to the public key passed in the identity-sequence certificate and thereby authenticate the unit as the one bearing the identity sequence included in the certificate.

34. (Canceled)

7

35. (Original) A configuration service system according claim 31 intended for use with a communications infrastructure comprising a data network, and an access network to which the user has a subscriber connection and which provides access to the data network through a data-network access point; the configuration service system having its interface means connected to the data network and further comprising an authorisation server for providing a logon authorisation service to said data-network access point in respect of connectivity units requesting access to the configuration service system through that access point.

36. (Previously presented) A configuration service system according to claim 31, further comprising means for sending a wakeup indication to said connectivity unit for causing the latter to contact said service entity, the data processing system, after transmitting said operational communications parameters to the connectivity unit, triggering the wakeup means to send a said wakeup indication to the connectivity unit after the latter has terminated its communication with the data processing system.

37. (Original) A configuration service system according claim 36, wherein the communications infrastructure comprises a data network to which the interface means of the configuration service system is connected, and an access network to which the user has a subscriber connection and which provides access to the data network through a data-network access point; said user-related information held in said store including an identifier of the subscriber connection on said access network and said wake-up indication placed by the wakeup means taking the form of a call to said subscriber connection.

38. (Previously presented) A connectivity unit for communicating with a service entity across a communications infrastructure, said connectivity unit comprising:
- a store holding configuration communications parameters including a public-key / private-key cryptographic key pair with an identity-sequence

8

certificate linking the public key to an identity sequence specific to the connectivity unit;

- communication means for establishing communication across said communications Infrastructure with a remote entity In accordance with communications parameters held in said store, the communications means including authentication means for authenticating the connectivity unit to the remote entity, the authentication means comprising means for passing a key certificate to the remote entity, and

- configuration initiation means for causing the communication means to establish communication across said communications infrastructure with a configuration service by using said configuration communications parameters held in said store, the said key certificate used by the authentication means being the identity-sequence certificate;

- download means for downloading operational communications parameters from the configuration service and storing them in said store; and

- operational control means for causing the communication means to establish communication across said communications infrastructure with said service entity by using said operational communications parameters held in said store;

said operational communications parameters including a user-identity certificate linking the said public key to the identity of a user associated with connectivity unit, the user-identity certificate being used as said key certificate by the authentication means for authenticating the connectivity unit to the service entity upon the operational control means causing the communication means to establish communication with the service entity.

39. (Original) A connectivity unit according to claim 38, wherein said authentication means further comprises means for generating and returning a response to a challenge issued by the remote entity, the generation of the response Involving the use of said private key to effect a cryptographic operation on data included in the challenge.

9

40. (Original) A connectivity unit according to claim 38, wherein said configuration initiation means is responsive to the absence of valid operational communications parameters in said store upon the connectivity unit being powered up and connected to the communications infrastructure, to automatically trigger the communication means to establish communications with the configuration service without requiring the input of data by a user.

41. (Original) A connectivity unit according to claim 38, wherein the communication means is operative to establish communication across a communications infrastructure that comprises a data network, and an access network to which the user of the connectivity unit has a subscriber connection and which provides access to the data network through a data-network access point, access to the data network through said data-network access point being subject to a username/password authorisation process; said configuration communications parameters held in said store further including the access-network address of the data-network access point and a username and password for use in said authorisation process, said username including said identity sequence specific to the connectivity unit.

42. (Original) A connectivity unit according to claim 41, wherein the username included in said configuration communications parameters is of the form:

identity sequence of connectivity unit @ configuration_domain

where the configuration_domain serves to indicate to the data-network access point an authorisation server to be used in the authorisation process.

43-44. (Canceled)

45. (Previously presented) A method of configuring a connectivity unit for communication with a service entity, comprising the steps of:

10

(A) - prior to a user taking possession of the unit, pre-installing in the unit a public-key/private-key cryptographic key pair and configuration communication parameters including an identity-sequence certificate linking the public key to an identity sequence of the unit;

(B) - storing user-related information for access by a configuration service;

(C) - establishing a connection between the connectivity unit and the configuration service using the configuration communication parameters, using the identity-sequence certificate to authenticate the unit to the configuration service, and transferring from the service to the unit operational communication parameters including a user-id certificate associating the public key of the unit with a user identity derived from said user-related information; and

(D) -   subsequently using the operational communication parameters to establish communication between the connectivity unit and service entity with the user-id certificate being used to authenticate the unit to the entity.

46. (Previously presented) A method of configuring a connectivity unit for communication with a service entity, comprising:

initially installing in said unit a public-key/private-key cryptographic key pair and an identity-sequence certificate linking the public key to an identity sequence of the unit;

storing user-related information for access by a configuration service;

establishing a connection between said unit and said configuration service, using the identity-sequence certificate to authenticate the unit to the service, and transferring from the service to the unit communication parameters including a user-id certificate associating said public key with a user identity derived from said user-related information; and

subsequently establishing communication between said unit and a service entity using said communication parameters and using the user-id certificate to authenticate the unit to the entity.